OIPE
FEB 19 2003
PATENT & TRADEMARK OFFICE

Clean Copy of Amended Claims

RECEIVED
FEB 20 2003
Technology Center 2100

OIPE
FEB 19 2003
PATENT & TRADEMARK OFFICE

1. (AMENDED) A data processing apparatus for processing content data provided by a recording or communication medium, said apparatus comprising:

a cryptography process section for executing a cryptography process on said content data; and

a control section for executing control for said cryptography process section, wherein said cryptography process section:

generates partial integrity check values as integrity check values for a partial data set, said partial data set containing partial data obtained by a content data-constituting section,

collates said integrity check values to verify said partial data,

generates an intermediate integrity check value based on a partial integrity check value set containing at least one of said partial integrity check values, and

uses said intermediate integrity check value to verify the said partial data set.

2. (AMENDED) The data processing apparatus according to Claim 1, wherein:

said partial integrity check values are generated by means of said cryptography process with a partial-check-value-generating key applied thereto, using said partial data as a message;

said intermediate integrity check value is generated by means of said cryptography process with a general-check-value-generating key applied thereto, using said partial integrity check value set as said message; and

said cryptography process section is configured to store said partial-check-value-generating key and said general-check-value-generating key.

3. (AMENDED) The data processing apparatus according to Claim 1, wherein said cryptography process has plural types of partial-check-value-generating keys corresponding to said partial integrity check values.

4. (AMENDED) The data processing apparatus according to Claim 2, wherein:

said cryptography process is a DES cryptography process, and

said cryptography process section is configured to execute said DES cryptography process.

5. (AMENDED) The data processing apparatus according to Claim 2, wherein:

said partial integrity check values are message authentication codes generated in a DES-CBC mode using said partial data to be checked as said message;

said intermediate integrity check value is one of said message authentication codes generated in said DES-CBC mode using said partial integrity check value set as said message, and

said cryptography process section is configured to execute said cryptography process in said DES-CBS mode.

6. (AMENDED) The data processing apparatus according to Claim 5, wherein Triple DES is applied in part of a message string to be processed in said DES-CBC mode.

7. (AMENDED) The data processing apparatus according to Claim 1, further comprising:

a signature key wherein: said cryptography process section is configured to apply a value generated from said intermediate integrity check value by means of said signature key as a collation value for data verification.

8. (AMENDED) The data processing apparatus according to Claim 7, wherein:

said signature key includes a plurality of different signature keys; and

said cryptography process section is configured to apply one of said plurality of different signature keys, which is selected depending on a localization of said content data, to said cryptography process for said intermediate integrity check value to obtain said collation value for data verification.

9. (AMENDED) The data processing apparatus according to Claim 8, further comprising:

a common signature key common to all entities of a system for executing a data verifying process; and

an apparatus-specific signature key specific to each apparatus that executes said data verifying process.

10. (AMENDED) The data processing apparatus according to Claim 1, wherein:

said partial integrity check values contain at least one header section integrity check value and at least one content integrity check value, said at least one header section integrity check value being generated for intra-header-section data partly constituting data and said at least one content integrity check value being generated for content block data partly constituting said data; and

said cryptography process is configured to generate at least one header section integrity check value for said partial data set in said intra-header-section data to execute a collation process, generate at least one content integrity check value for said partial data set in said intra-content-section data to execute said collation process, and further

generate a general integrity check value based on all of said header section integrity check values and said content integrity check values to execute said collation process in order to verify said data.

11. (AMENDED) The data processing apparatus according to Claim 1, wherein:

said partial integrity check values contain at least one header section integrity check value generated for intra-header-section data partly constituting data; and

said cryptography process is configured to generate at least one header section integrity check value for said partial data set in said intra-header-section data to execute a collation process and further generate a general integrity check value based on said at least one header section integrity check value and on content block data constituting part of said data, to execute said collation process in order to verify said data.

12. (AMENDED) The data processing apparatus according to Claim 1, further comprising a recording device for storing data validated by said cryptography process section.

13. (AMENDED) The data processing apparatus according to Claim 12, wherein:

said control section suspends storing of said data in said recording device if a process of collating said partial integrity check values is not established in said cryptography process executed by said cryptography process section.

14. (AMENDED) The data processing apparatus according to Claim 1, further comprising a reproduction process section for

reproducing data validated by said cryptography process section.

15. (AMENDED) The data processing apparatus according to Claim 14, wherein:

said control section suspends reproducing of said data in said reproduction process section if a process of collating said partial integrity check values is not established in said cryptography process executed by said cryptography process section.

16. (AMENDED) The data processing apparatus according to Claim 14, further comprising:

control means for collating only header section integrity check values in said data during said cryptography process executed by said cryptography process section to collate said partial integrity check values; and

transmitting to said reproduction process section said data for which collation of said header section integrity check values has been established.

17. (AMENDED) A data processing apparatus for processing content data provided by a recording or communication medium, said apparatus comprising:

a cryptography process section for executing a cryptography process on said content data; and

a control section for executing control for said cryptography process section, wherein

if data to be verified is encrypted data said cryptography process section generates integrity check values for said data by means of a signature data-applied cryptography process on arithmetic operation results obtained by executing an arithmetic operation process on decrypted data

obtained by executing a decryption process on said encrypted data.

18. (AMENDED) The data processing apparatus according to Claim 17, wherein said arithmetic operation process comprises performing an exclusive-OR operation on said decrypted data at predetermined bytes, said decrypted data being obtained by decrypting said encrypted data.

19. (AMENDED) A data processing method for processing content data provided by a recording or communication medium, said method comprising:

generating partial integrity check values as integrity check values for a partial data set, said partial data set containing partial data obtained by a content data-constituting section;

collating said integrity check values to verify said partial data;

generating an intermediate integrity check value based on a partial integrity check value set containing at least one of said partial integrity check values; and

verifying said partial data set corresponding to said partial integrity check values using said intermediate integrity check value.

20. (AMENDED) The data processing method according to Claim 19, wherein:

said partial integrity check values are generated by means of a cryptography process with a partial-check-value-generating key applied thereto, using said partial data as a message; and

said intermediate integrity check value is generated by means of said cryptography process with a general-check-

value-generating key applied thereto, using said partial integrity check value set as said message.

21. (AMENDED) The data processing method according to Claim 20, wherein said partial integrity check values are generated by applying different types of said partial-check-value-generating key corresponding to partial integrity check values.

22. (AMENDED) The data processing method according to Claim 20, wherein said cryptography process is a DES cryptography process.

23. (AMENDED) The data processing method according to Claim 19, wherein:

said partial integrity check values include a message authentication code generated in a DES-CBC mode using said partial data as a message; and

said intermediate integrity check value is said message authentication code generated in said DES-CBC mode using said partial integrity check value set as said message.

24. (AMENDED) The data processing method according to Claim 19, wherein a value generated from said intermediate integrity check value by means of a signature key-applied cryptography process is applied as a collation value for data verification.

25. (AMENDED) The data processing method according to Claim 24, wherein different signature keys are applied to said cryptography process for said intermediate integrity check value depending on a localization of content data, said different signature keys being applied to obtain said collation value for data verification.

26. (AMENDED) The data processing method according to Claim 25, further comprising:

selecting and using one of

a common signature key common to all entities of a system for executing a data verifying process; and

an apparatus-specific signature key specific to each apparatus that executes said data verifying process,

said selecting step being based on the localization of said content data.

27. (AMENDED) The data processing method according to Claim 19, wherein

said partial integrity check values contain at least one header section integrity check value generated for intra-header section data partly constituting data and at least one content integrity check value generated for intra-content section data partly constituting said data; and said method further comprising:

generating at least one header section integrity check value for said partial data set in said intra-header-section data to execute a collation process;

generating at least one content integrity check value for said partial data set in said intra-content-section data to execute said collation process; and

generating a general integrity check value based on all of said header section integrity check values and said content integrity check values, said general integrity check value being operable to execute said collation process in order to verify said data.

28. (AMENDED) The data processing method according to Claim 19, wherein:

said partial integrity check values contain at least one header section integrity check value generated for intra-

header section data partly constituting data, said method further comprising:

generating at least one header section integrity check value for said partial data set in said intra-header-section data to execute a collation process; and

generating a general integrity check value based on said at least one header section integrity check value and on content block data constituting part of said data, said general integrity check value being operable to execute said collation process in order to verify said data.

29. (AMENDED) The data processing method according to Claim 19, further comprising storing validated data after verifying said partial data set.

30. (AMENDED) The data processing method according to Claim 29, further comprising suspending said storing of said validated data if collating of said partial integrity check values is not established.

31. (AMENDED) The data processing method according to Claim 19, further comprising: reproducing data after verifying said partial data set.

32. (AMENDED) The data processing method according to Claim 31, further comprising:

suspending said reproducing of said data if collating of said partial integrity check values is not established.

33. (AMENDED) The data processing method according to Claim 31, wherein:

said collating of said partial integrity check values only collates header section integrity check values and transmits said data for which collation of said header section integrity check values has been established to a reproduction process section for reproduction.

34. (AMENDED) A data processing method for processing content data provided by a recording or communication medium, the method comprising:

decrypting encrypted data to be verified to obtain decrypted data;

executing an arithmetic operation process on said decrypted data to obtain results ; and

executing a signature key-applied cryptography process on said results to generate integrity check values for said data to be verified.

35. (AMENDED) The data processing method according to Claim 34, wherein said arithmetic operation process comprises performing an exclusive-OR operation on said decrypted data at predetermined bytes.

36. (AMENDED) A data verifying value imparting method for a data verifying process, said method comprising:

imparting partial integrity check values as integrity check values for a partial data set, said partial data set containing partial data obtained by a content data-constituting section; and

imparting an intermediate integrity check value to data to be verified, said intermediate integrity check value being used to verify a partial integrity check value set containing at least one of said partial integrity check values.

37. (AMENDED) The data verifying value imparting method according to Claim 36, wherein:

said partial integrity check values are generated by means of a cryptography process with a partial-check-value-generating key applied thereto, using said partial data as a message; and

said intermediate integrity check value is generated by means of said cryptography process with a general-check-value-generating key applied thereto, using said partial integrity check value set as said message.

38. (AMENDED) The data verifying value imparting method according to Claim 37, wherein said partial integrity check values are generated by applying different types of said partial-check-value-generating key corresponding to said partial integrity check values.

39. (AMENDED) The data verifying value imparting method according to Claim 37 wherein said cryptography process is a DES cryptography process.

40. (AMENDED) The data verifying value imparting method according to Claim 36, wherein:

said partial integrity check values include a message authentication code generated in a DES-CBC mode using said partial data as a message; and

said intermediate integrity check value is said message authentication code generated in said DES-CBC mode using said partial integrity check value set as said message.

41. (AMENDED) The data verifying value imparting method according to Claim 36 wherein a value generated from said intermediate integrity check value by means of a signature

key-applied cryptography process is applied as a collation value for data verification.

42. (AMENDED) The data verifying value imparting method according to Claim 41, wherein different signature keys are applied to said cryptography process for said intermediate integrity check value to obtain said collation value, said different signature keys being applied depending on a localization of content data.

43. (AMENDED) The data verifying value imparting method according to claim 42, further comprising:

selecting either a common signature key or an apparatus-specific signature key as one of said different signature keys depending upon the localization of said content data, said common signature key being common to all entities of a system for executing said data verifying process, and said apparatus-specific signature key being specific to each apparatus that executes said data verifying process.

44. (AMENDED) The data verifying value imparting method according to Claim 36, wherein:

said partial integrity check values contain at least one header section integrity check value for intra-header section data partly constituting data and at least one content integrity check value generated for intra-content-section data partly constituting said data,

said method further comprising:

generating a general integrity check value to verify said data for said at least one header section integrity check value and said at least one content integrity check value.

45. (AMENDED) The data verifying value imparting method according to Claim 36, wherein:

said partial integrity check values contain at least one header section integrity check value for intra-header-section data partly constituting data,

said method further comprising:

generating a general integrity check value to verify said data, said general integrity check value being generated for said at least one header section integrity check value and content block data partly constituting said data.

46. (AMENDED) A recording medium recorded with a computer program for executing a data verifying process having certain actions, said actions comprising:

executing a collation process using partial integrity check values generated as integrity check values for a partial data set containing partial data; and

using an intermediate integrity check value to verify said partial data set, said intermediate integrity check value being based on a partial integrity check value set obtained by combining at least some of said partial integrity check values together, and said partial data set corresponding to said partial integrity check values constituting said partial integrity check value set.

47. (AMENDED) A data processing apparatus, comprising:

an encryption processing section that executes encryption processing including at least one of data encryption, data decryption, data verification, authentication processing and signature processing; and

a storage section that stores master keys to generate keys used for said encryption processing,

wherein said encryption processing section is configured to generate individual keys for executing said

encryption processing based on one of said master keys, an encryption processing target apparatus, and data identification data.

48. (AMENDED) The data processing apparatus according to Claim 47, wherein:

said encryption processing section performs said encryption processing on transfer data via a storage medium or a communication medium;

said storage section stores a distribution key generation master key MKdis for generating a distribution key Kdis, said distribution key Kdis being used for said encryption processing of said transfer data; and

said encryption processing section executes said encryption processing based on said distribution key generation master key MKdis and a data identifier, said data identifier including identification data of said transfer data.

49. (AMENDED) The data processing apparatus according to Claim 47, wherein:

said data processing apparatus performs authentication processing of an externally connected apparatus which data is transferred to or from;

said storage section stores an authentication key generation master key MKake for generating an authentication key Kake of said externally connected apparatus; and

said encryption processing section executes said encryption processing based on said authentication key generation master key MKake and an externally connected apparatus identifier, said externally connected apparatus identifier including identification data of said externally connected apparatus.

50. (AMENDED) The data processing apparatus according to Claim 47, wherein:

said encryption processing section performs said signature processing on data;

said storage section stores a signature key generation master key MKdev for generating a data processing apparatus signature key Kdev of said data processing apparatus; and

said encryption processing section executes said signature processing based on said signature key generation master key MKdev and a data processing apparatus identifier, said data processing apparatus identifier including identification data of said data processing apparatus.

51. (AMENDED) The data processing apparatus according to Claim 47, wherein said encryption processing section performs individual key generation processing to generate said individual keys for executing said encryption processing based on said master keys and identification data, said encryption processing using said identification data as a message and applying said master keys as encryption keys.

52. (AMENDED) The data processing apparatus according to Claim 51, wherein said encryption processing uses a DES algorithm.

53. (AMENDED) A data processing system, comprising:

a plurality of data processing apparatuses;

a common master key to generate a key used for encryption processing including at least one of data encryption, data decryption, data verification, authentication processing and signature processing, each of said plurality of data processing apparatuses having said common master key; and

a common individual key for executing said encryption processing based on said master key and identification data, each of said plurality of data processing apparatuses generating said common individual key.

54. (AMENDED) The data processing system according to Claim 53, further comprising:

a contents data providing apparatus operable to configure said plurality of data processing apparatuses and to supply contents data; and

a contents data utilization apparatus that utilizes said contents data,

both said contents data providing apparatus and said contents data utilization apparatus having a distribution key generation master key to generate a contents data distribution key, said contents data distribution key being used for said encryption processing of circulation contents data between said contents data providing apparatus and said contents data utilization apparatus,

said contents data providing apparatus generating said contents data distribution key based on said distribution key generation master key and a contents identifier, said contents identifier being an identifier of said contents data, and

said contents data utilization apparatus generating said contents data distribution key based on said distribution key generation master key and said contents identifier.

55. (AMENDED) The data processing system according to Claim 54, wherein:

said contents data providing apparatus generates a plurality of different contents data distribution keys based on a plurality of different distribution key generation master keys and said contents identifier, executes said encryption

processing using said plurality of different contents data distribution keys, and generates encryption contents data having a plurality of types, and

said contents data utilization apparatus has at least one of said e plurality of different distribution key generation master keys, and makes decodable only said encryption contents data formed by a distribution key generated using one of said different distribution key generation master keys that is the same as a distribution key generation master key owned by an apparatus.

56. (AMENDED) The data processing system according to Claim 53, further including:

a contents key generation master key to generate a contents key used for said encryption processing of contents data, said contents key generation master key being stored in each of said plurality of data processing apparatuses;

a first one of said plurality of data processing apparatuses storing said contents data in a storage medium, said contents data being encrypted by said contents key and an apparatus identifier of said first one of said plurality of data processing apparatuses; and

a second one of said plurality of data processing apparatuses generating said contents key based on said contents key generation master key and said apparatus identifier of said first one of said plurality of data processing apparatuses, and executing decryption processing on said contents data stored in said storage medium.

57. (AMENDED) The data processing system according to Claim 53, further including:

a host device having an authentication key generation master key; and

a slave device subject to authentication processing by said host device, said slave device having said authentication key generation master key and a slave device identifier, said authentication key generation master key being used for authentication processing between said host device and said slave device, wherein:

said slave device generates an authentication key based on said authentication key generation master key and said slave device identifier, said slave device identifier being an identifier of said slave device and being stored in a memory of said slave device,

said host device generates said authentication key based on said authentication key generation master key and said slave device identifier, and

said plurality of data processing apparatuses are configured by said host device and said slave device.

58. (AMENDED) A data processing method that executes encryption processing including at least one of data encryption, data decryption, data verification, authentication processing and signature processing, said data processing method comprising:

generating individual keys based on master keys and identification data of an externally connected apparatus or data subject to said encryption processing; and

executing said encryption processing based on said individual keys.

59. (AMENDED) The data processing method according to Claim 58, wherein said encryption processing is executed on transfer data via a storage medium or a communication medium;

said step of generating said individual keys includes executing encryption processing based on a distribution key generation master key MKdis and a data

identifier, and generating a distribution key Kdis of said transfer data, said distribution key Kdis being used for encryption processing of said transfer data, and said data identifier including said identification data of said transfer data; and

said encryption processing step includes executing encryption processing on said transfer data based on said distribution key Kdis.

60. (AMENDED) The data processing method according to Claim 58, wherein:

said encryption processing is authentication processing of the externally connected apparatus to and from which said data is transferred;

said step of generating said individual keys includes executing said encryption processing and generating an authentication key Kake, said encryption processing being based on an authentication key generation master key MKake and an externally connected apparatus identifier, said externally connected apparatus identifier including said identification data of said externally connected apparatus; and

said step of executing said encryption processing includes executing said authentication processing of said externally connected apparatus based on said authentication key Kake.

61. (AMENDED) The data processing method according to Claim 58, wherein:

said encryption processing is said signature processing on said data;

said step of generating said individual keys includes executing said signature processing based on a signature key generation master key Mkdev and a data processing apparatus identifier, and generating a data

processing apparatus signature key Kdev of a data processing apparatus, said signature key generation master key Mkdev being operable to generate said data processing apparatus signature key Kdev, and said data processing apparatus identifier being identification data of said data processing apparatus; and

said encryption processing includes executing said signature processing on said data based on said signature key Kdev.

62. (AMENDED) The data processing method according to Claim 58, wherein said step of generating said individual keys includes executing said encryption processing using at least part of said data identification of said externally connected apparatus or said data subject to said encryption processing as a message, and applying said master keys as encryption keys.

63. (AMENDED) The data processing method according to Claim 62, wherein said encryption processing uses a DES algorithm.

64. (AMENDED) A data processing system, comprising:

a contents data providing apparatus that supplies contents data, said contents data providing apparatus being operable to generate a contents data distribution key based on a distribution key generation master key and a contents identifier, said contents identifier being an identifier of said contents data and said contents data providing apparatus being operable to execute encryption processing on said contents data; and

a contents data utilization apparatus that utilizes said contents data, said contents data utilization apparatus being operable to generate said contents data distribution key

based on said distribution key generation master key and said contents identifier.

65. (AMENDED) The data processing system according to Claim 64, wherein:

said contents data providing apparatus generates a plurality of different contents data distribution keys based on a plurality of different distribution key generation master keys and said contents identifier, executes said encryption processing using said plurality of different contents data distribution keys, and generates encryption contents data having a plurality of types; and

said contents data utilization apparatus has at least one of said plurality of different distribution key generation master keys, and decrypts only said encryption contents data formed by a distribution key generated using one of said different distribution key generation master keys that is the same as a distribution key generation master key owned by an apparatus.

66. (AMENDED) A data processing method in a data processing system configured by a plurality of data processing apparatuses, said method comprising:

storing contents data in a storage medium, said contents data being encrypted using a contents key and being stored by a data processing apparatus A, and said contents key being generated based on a contents data generation master key and an apparatus identifier of said data processing apparatus A;

generating said contents key with a data processing apparatus B based on said contents key generation master key and said apparatus identifier; and

decrypting said contents data stored in said storage medium using said contents key generated by said data processing apparatus B.

67. (AMENDED) A data processing method in a data processing system including a host device and a slave device subject to authentication processing by said host device, said data processing method comprising:

generating an authentication key in said slave device based on an authentication key generation master key and a slave device identifier, said authentication key being used for said authentication processing between said host device and said slave device, said slave device identifier being an identifier of said slave device;

storing said authentication key in a memory in said slave device;

generating said authentication key in said host device based on said authentication key generation master key and said slave device identifier; and

executing said authentication processing.

68. (AMENDED) A recording medium recorded with a computer program for executing encryption processing having certain actions to perform at least one of data encryption, data decryption, data verification, authentication processing and signature processing on a computer system, said actions comprising:

generating individual keys based on master keys and identification data; and

executing said encryption processing based on said individual keys.

69. (AMENDED) A data processing apparatus that processes contents data supplied from a storage medium or communication medium, comprising:

a storage section that stores data processing apparatus identifiers;

a list verification section that extracts an illegal device list included in said contents data and executes collation between entries in said illegal device list and said data processing apparatus identifiers stored in said storage section; and

a control section that terminates processing of at least one of reproduction of said contents data or processing of storage in a recording device when a result of said collation shows that said illegal device list includes information that matches said data processing apparatus identifiers.

70. (AMENDED) The data processing apparatus according to Claim 69, wherein:

said list verification section comprises an encryption processing section that executes encryption processing on said contents data; and

said encryption processing section verifies the presence or absence of tampering in said illegal device list based on check values of said illegal device list included in said contents device and executes said collation only when said verification proves no tampering.

71. (AMENDED) The data processing apparatus according to Claim 70, further comprising an illegal device list check value generation key, wherein said encryption processing section executes said encryption processing by applying said illegal device list check value generation key to illegal device list configuration data to be verified, generates

illegal device list check values, executes collation between said illegal device list check values and illegal device list check values included in said contents data and thereby verifies the presence or absence of tampering in said illegal device list.

72. (AMENDED) The data processing apparatus according to Claim 69, wherein:

said list verification section comprises an encryption processing section that executes encryption processing on said contents data; and

said encryption processing section executes decryption processing of an encrypted illegal device list included in said contents data to produce a decrypted illegal device list, and executes said collation on said decrypted illegal device list.

73. (AMENDED) The data processing apparatus according to Claim 69, wherein:

said list verification section comprises an encryption processing section that executes mutual authentication processing with a recording device to which and from which said contents data is transferred; and

said list verification section extracts said illegal device list included in said contents data and executes said collation with said data processing apparatus identifiers stored in said storage section on condition that authentication with said recording device has been established through said mutual authentication processing executed by said encryption processing section.

74. (AMENDED) A data processing method that processes contents data supplied from a storage medium or communication medium, comprising:

extracting an illegal device list included in said contents data;

executing collation between entries included in said illegal device list and data processing apparatus identifiers stored in a storage section in a data processing apparatus; and

stopping execution of processing of at least one of reproduction of said contents data or processing of storage in a recording device when a result of said collation step shows that said illegal device list includes information that matches said data processing apparatus identifiers.

75. (AMENDED) The data processing method according to Claim 74, further comprising

verifying the presence or absence of tampering in said illegal device list based on check values of said illegal device list included in said contents data; and

executing said collation only when said verifying step proves no tampering.

76. (AMENDED) The data processing method according to Claim 75, wherein said verifying step includes:

executing encryption processing by applying an illegal device list check value generation key to illegal device list configuration data to be verified and generating illegal device list check values; and

executing collation between said illegal device list check values and said illegal device list check values included in said contents data and thereby verifying the presence or absence of tampering in said illegal device list.

77. (AMENDED) The data processing method according to Claim 74, further comprising executing decrypting processing on an

encrypted illegal device list included in said contents data to produce a decrypted illegal device list; and

executing said collation on said decrypted illegal device list.

78. (AMENDED) The data processing method according to Claim 74, further comprising

executing mutual authentication processing with a recording device to which and from which said contents data is transferred, wherein

said collation is performed on condition that authentication with said recording device has been established through said mutual authentication processing step.

79. (AMENDED) A contents data generation method, comprising:

generating contents data to a plurality of recorders or a plurality of reproducers, said contents data being supplied from a storage medium or a communication medium; and

storing an illegal device list as the header information of the contents data, said illegal device list having component data comprising identifiers of said plurality of recorders or said plurality of reproducers,

whereby said illegal device list will be excluded from the use of said contents data.

80. (AMENDED) The contents data generation method according to Claim 79, wherein illegal device list check values for a tampering check on said illegal device list are stored as said header information of said contents data.

81. (AMENDED) The contents data generation method according to Claim 79, wherein said illegal device list is encrypted and stored in said header information of said contents data.

82. (AMENDED) A recording medium recorded with a computer program for processing of contents data supplied from a storage medium or a communication medium, said computer program comprising:

extracting an illegal device list included in said contents data;

executing collation between entries included in said illegal device list and data processing apparatus identifiers stored in a storage section in a data processing apparatus; and

stopping execution of processing of at least one of reproduction of said contents data or processing of storage in a recording device when a result of said collation step shows that said illegal device list includes information that matches said data processing apparatus identifiers.

83. (AMENDED) A data processing apparatus that processes contents data supplied via a recording medium or a communication medium, comprising:

an encryption processing section that executes encryption processing on said contents data;

a control section that executes control over said encryption processing section;

a system common key used for said encryption processing which is common to a plurality of data processing apparatuses using said contents data, said plurality of data processing apparatuses including said data processing apparatus; and

at least one of an apparatus-specific keyand an apparatus-specific identifier, said apparatus-specific key being specific to said data processing apparatus and said apparatus-specific identifier being used to generate said apparatus-specific key, wherein

said encryption processing section is configured to perform said encryption processing by applying one of said system common key and said apparatus-specific key according to a utilization mode of said contents data.

84. (AMENDED) The data processing apparatus according to Claim 83, wherein said encryption processing section executes said encryption processing by applying said one of said system common key and said apparatus-specific key according to utilization restriction information included in said contents data.

85. (AMENDED) The data processing apparatus according to Claim 83, further including a recording device for recording said contents data, wherein:

when said utilization mode restricts usage of said contents data to said data processing apparatus, data to be stored in said recording device is generated by executing said encryption processing using said apparatus-specific on said contents data; and

where said utilization mode permits usage of said contents data by at least one of said plurality of data processing apparatuses other than said data processing apparatus, said data is generated by executing said encryption processing using said system common key on said contents data.

86. (AMENDED) The data processing apparatus according to Claim 83, further including a signature key Kdev and a system signature key Ksys, said signature key Kdev being specific to said data processing apparatus and said system signature key Ksys being common to said plurality of data processing apparatuses, wherein:

when said contents data is stored in a recording device, said contents data being restricted to use by said

data processing apparatus, said encryption processing section generates an apparatus-specific check value through said encryption processing by applying said signature key Kdev to said contents data;

when said contents data is stored in said recording device, said contents data being available for use by at least one of said plurality of data processing apparatuses other than said data processing apparatus, said encryption processing section generates an overall check value through said encryption processing by applying said system signature key Ksys to said contents data; and

said control section performs control of storing said contents data in said recording device together with one of said apparatus-specific check value and said overall check value.

87. (AMENDED) The data processing apparatus according to Claim 83, further including a signature key Kdev and a system signature key Ksys, said signature key Kdev being specific to said data processing apparatus and said system signature key Ksys being common to said plurality of data processing apparatuses, wherein:

when said utilization mode restricts usage of said contents data to said data processing apparatus, and said contents data is reproduced, said encryption processing section generates an apparatus-specific check value by applying said signature key Kdev to said contents data and performing collation processing on said apparatus-specific check value;

when said utilization mode permits usage of said contents data by at least one of said plurality of data processing apparatuses other than said data processing apparatus, and said contents data is reproduced, said encryption processing section generates an overall check value

by applying said system signature key Ksys to said contents data and performing collation processing on said overall check value; and

said control section generates reproducible decrypted data by continuing processing of said contents data by the encryption processing section only when said collation processing on said apparatus-specific check value is established or when said collation processing on said overall check value is established.

88. (AMENDED) The data processing apparatus according to Claim 83, further including a data processing apparatus signature key master key MKdev and a data processing apparatus identifier IDdev, wherein

said encryption processing section generates a signature key Kdev through said encryption processing based on said data processing apparatus signature key master key MKdev and said data processing apparatus identifier IDdev.

89. (AMENDED) The data processing apparatus according to Claim 88, wherein said encryption processing section generates said signature key Kdev through DES encryption processing by applying said data processing apparatus signature key master key MKdev to said data processing apparatus identifier IDdev.

90. (AMENDED) The data processing apparatus according to Claim 83, wherein said encryption processing section generates an intermediate integrity check value by executing said encryption processing on said contents data, said encryption processing including applying one of said apparatus-specific key and said system common key to said intermediate integrity check value.

91. (AMENDED) The data processing apparatus according to Claim 90, wherein said encryption processing section generates a partial integrity check value through said encryption processing on a partial data set containing at least one partial data item obtained by dividing said contents data into a plurality of parts and generates said intermediate integrity check value through said encryption processing on a partial integrity check value set data string containing said partial integrity check value.

92. (AMENDED) A data processing method for a data processing apparatus that processes contents data supplied via a recording medium or a communication medium, said method comprising:

selecting, according to a utilization mode of said contents data, an encryption processing key from among an encryption processing system common key and an apparatus-specific key, said encryption processing system common key being common to a plurality of data processing apparatuses using said contents data, said plurality of data processing apparatuses including said data processing apparatus, and said apparatus-specific key being specific to said data processing apparatus; and

executing encryption processing by applying said encryption processing key to said contents data.

93. (AMENDED) The data processing method according to Claim 92, wherein said step of selecting said encryption processing key includes selecting said encryption processing key according to utilization restriction information contained in said contents data.

94. (AMENDED) The data processing method according to Claim 92, further including:

generating data to be stored in a recording device by executing said encryption processing using said apparatus-specific key on said contents data when said utilization mode restricts usage of said contents data to said data processing apparatus; and

, generating said data to be stored in said recording device by executing said encryption processing using said encryption processing system common key on said contents data when said utilization mode permits usage of said contents data by at least one of said plurality of data processing apparatuses other than said data processing apparatus.

95. (AMENDED) The data processing method according to Claim 92, further including:

generating an apparatus-specific check value through said encryption processing by applying an apparatus-specific signature key Kdev to said contents data when said contents data is restricted to use by said data processing apparatus and is stored in said recording device;

generating an overall check value through said encryption processing by applying a system signature key Ksys to said contents data when said contents data is available for use by at least one of said plurality of data processing apparatuses other than said data processing apparatus and is stored in said recording device; and

storing said contents data in said recording device together with one of said apparatus-specific check value and said overall check value.

96. (AMENDED) The data processing method according to Claim 92, further including:

when reproducing said contents data, wherein said utilization mode restricts usage of said contents data by said data processing apparatus:

generating an apparatus-specific check value through said encryption processing by applying an apparatus-specific signature key Kdev to said contents data, and

performing collation processing on said apparatus-specific check value;

when reproducing said contents data, wherein said utilization mode permits usage of said contents data by at least one of said plurality of data processing apparatuses other than said data processing apparatus:

generating an overall check value through said encryption processing by applying a system signature key Ksys to said contents data, and

performing collation processing on said overall check value; and

reproducing said contents data only when said collation processing on said apparatus-specific check value is established or when said collation processing on said overall check value is established.

97. (AMENDED) The data processing method according to Claim 92, further comprising generating a signature key Kdev through said encryption processing based on a data processing apparatus signature key master key MKdev and a data processing apparatus identifier IDdev.

98. (AMENDED) The data processing method according to Claim 97, wherein said step of generating said signature key Kdev includes DES encryption processing by applying said data processing apparatus signature key master key MKdev to said data processing apparatus identifier IDdev.

99. (AMENDED) The data processing method according to Claim 92, further comprising generating an intermediate integrity check value by executing said encryption processing

on said contents data, said encryption processing including applying one of said apparatus-specific key and said system common key to said intermediate integrity check value.

100. (AMENDED) The data processing method according to Claim 99, further including:

generating a partial integrity check value through said encryption processing on a partial data set containing at least one partial data item obtained by dividing said contents data into a plurality of parts; and

generating said intermediate integrity check value through said encryption processing on a partial integrity check value set data string containing said partial integrity check value.

101. (AMENDED) A recording medium recorded with a computer program for a data processing apparatus, said computer program processing contents data supplied via a recording medium or a communication medium, said computer program comprising:

selecting, according to a utilization mode of said contents data, a key from among an encryption processing key, an encryption processing system common key and an apparatus-specific key, said encryption processing system common key being common to a plurality of data processing apparatuses using said contents data, said plurality of data processing apparatuses including said data processing apparatus, and said apparatus-specific key being specific to said data processing apparatus; and

executing encryption processing by applying said key to said contents data.

102. (AMENDED) A data processing apparatus that processes contents data supplied via a recording medium or a communication medium, comprising:

an encryption processing section that executes encryption processing on said contents data, said encryption processing section being configured to generate a contents check value in units of contents block data included in said contents data and to execute collation processing on said contents check value and thereby execute verification processing as to the validity of each of said units of contents block data; and

a control section that executes control over said encryption processing section.

103. (AMENDED) The data processing apparatus according to Claim 102, further including a contents check value generation key, wherein said encryption processing section generates a contents intermediate value based on said contents block data and said encryption processing system generates said contents check value by applying said contents check value generation key to said contents intermediate value.

104. (AMENDED) The data processing apparatus according to Claim 103, wherein:

when said contents block data is encrypted, said encryption processing section generates said contents intermediate value by executing predetermined operation processing on an entire decrypted statement in units of a predetermined number of bytes, said entire decrypted statement being obtained by decryption processing of said contents block data; and

when said contents block data is not encrypted, said encryption processing section generates said contents intermediate value by executing said predetermined operation processing on said contents block data in said units of said predetermined number of bytes.

105. (AMENDED) The data processing apparatus according to Claim 104, wherein said predetermined operation processing is an exclusive-OR operation.

106. (AMENDED) The data processing apparatus according to Claim 104, wherein:

said encryption processing section has an encryption processing configuration in a CBC mode; and

said decryption processing is decryption processing in said CBC mode.

107. (AMENDED) The data processing apparatus according to Claim 106, wherein said encryption processing configuration in said CBC mode is a configuration in which common key encryption processing is applied a plurality of times only to part of a message string.

108. (AMENDED) The data processing apparatus according to Claim 102, wherein, when said contents block data contains a plurality of parts and a portion of said plurality of parts is to be verified, said encryption processing section generates said contents check value based on said portion to be verified, and executes said collation processing on said contents check value.

109. (AMENDED) The data processing apparatus according to Claim 108, wherein, when said portion is encrypted:

said encryption processing section generates said contents check value by applying a contents check value generation key to a value obtained by carrying out an exclusive-OR in units of a predetermined number of bytes on an entire decrypted statement, said entire decrypted statement being obtained by decryption processing of said portion; and

when said portion is not encrypted:

said encryption processing section generates said contents check value by applying said contents check value generation key to said value.

110. (AMENDED) The data processing apparatus according to Claim 108, wherein, when said portion of said plurality of parts needs to be verified, said encryption processing section applies a contents check value generation key to said portion of said plurality of parts to obtain a parts check value, applies said contents check value generation key to link data of said parts check value to obtain a result, and uses said result as said contents check value.

111. (AMENDED) The data processing apparatus according to Claim 102, wherein said encryption processing section further comprises a recording device for storing said contents data containing said units of contents block data whose validity has been verified.

112. (AMENDED) The data processing apparatus according to Claim 111, wherein, when said collation processing is not executed on said contents check value, said control section stops said storage in said recording device.

113. (AMENDED) The data processing apparatus according to Claim 102, wherein said encryption processing section further comprises a reproduction processing section for reproducing data whose validity has been verified.

114. (AMENDED) The data processing apparatus according to Claim 113, wherein, when said collation processing is not executed on said contents check value, said control section stops said reproduction in said reproduction processing section.

115. (AMENDED) A data processing method that processes contents data supplied via a recording medium or a communication medium, comprising:

generating a contents check value in units of contents block data included in said contents data; and

executing collation processing on said contents check value and thereby executing verification processing as to the validity of said units of contents block data.

116. (AMENDED) The data processing method according to Claim 115, further including:

generating a contents intermediate value based on said contents block data; and

generating said contents check value by executing encryption processing by applying said contents check value generation key to said contents intermediate value.

117. (AMENDED) The data processing method according to Claim 115, further including:

when said contents block data is encrypted, generating a contents intermediate value by executing predetermined operation processing on an entire decrypted statement in units of a predetermined number of bytes, said entire decrypted statement being obtained by decryption processing of said contents block data; and

when said contents block data is not encrypted, generating said contents intermediate value by executing said predetermined operation processing on said contents block data in said units of said predetermined number of bytes.

118. (AMENDED) The data processing method according to Claim 117, wherein said predetermined operation processing is an exclusive-OR operation.

119. (AMENDED) The data processing method according to Claim 117, wherein said decryption processing is decryption processing in a CBC mode.

120. (AMENDED) The data processing method according to Claim 119, wherein, in said step of decryption processing in said CBC mode, common key encryption processing is applied a plurality of times only to part of a message string.

121. (AMENDED) The data processing method according to Claim 115, further including, when said contents block data contains a plurality of parts and a portion of said plurality of parts is to be verified, generating said contents check value based on said portion to be verified prior to executing said collation processing on said contents check value.

122. (AMENDED) The data processing method according to Claim 121, further including:

when said portion is encrypted:

performing decryption processing of said portion to obtain an entire decrypted statement,

carrying out an exclusive-OR operation in units of a predetermined number of bytes on said entire decrypted statement, and

generating said contents check value by applying a contents check value generation key to a value obtained by said exclusive-OR operation; and

when said portion is not encrypted:

generating said contents check value by applying said contents check value generation key to said value.

123. (AMENDED) The data processing method according to Claim 121, further including:

applying a contents check value generation key to each of said plurality of parts to obtain a parts check value;

further applying said contents check value generation key to link data of said parts check value to obtain a result; and

using said result as said contents check value.

124. (AMENDED) The data processing method according to Claim 115, further including storing said contents data containing said units of contents block data whose validity has been verified.

125. (AMENDED) The data processing method according to Claim 124, further including stopping said storing of said contents data when said collation processing is not executed on said contents check value.

126. (AMENDED) The data processing method according to Claim 115, further including reproducing data whose validity has been verified.

127. (AMENDED) The data processing method according to Claim 126, further including stopping said reproduction when said collation processing is not executed on said contents check value.

128. (AMENDED) A contents data verification value assignment method for contents data verification processing, comprising:

generating a contents check value in units of contents block data, said contents block data being included in said contents data; and

assigning said contents check value to said contents data.

129. (AMENDED) The contents data verification value assignment method according to Claim 128, wherein said contents check value is generated through encryption processing by applying a contents check value generation key using said contents block data as a message.

130. (AMENDED) The contents data verification value assignment method according to Claim 128, wherein:

said contents check value is generated by generating a contents intermediate value based on said contents block data and applying a contents check value generation key to said contents intermediate value.

131. (AMENDED) The contents data verification value assignment method according to Claim 128, wherein said contents check value is generated by executing encryption processing on said contents block data in a CBC mode.

132. (AMENDED) The contents data verification value assignment method according to Claim 131, wherein said CBC mode is a configuration in which common key encryption processing is applied a plurality of times only to part of a message string.

133. (AMENDED) The contents data verification value assignment method according to Claim 128, wherein said contents block data contains a plurality of parts and a portion of said plurality of parts is to be verified, said method further comprising:

generating said contents check value based on said portion; and

assigning said contents check value to said contents data.

134. (AMENDED) The contents data verification value assignment method according to Claim 133, further including:

when said portion is encrypted:

performing decryption processing of said portion to obtain an entire decrypted statement,

carrying out an exclusive-OR operation in units of a predetermined number of bytes on said entire decrypted statement to obtain a value, and

generating said contents check value by applying a contents check value generation key to said value; and

when said portion is not encrypted:

generating said contents check value by applying said contents check value generation key to said value.

135. (AMENDED) The contents data verification value assignment method according to Claim 133, further including:

applying a contents check value generation key to each of said plurality of parts to obtain a parts check value;

further applying said contents check value generation key to link data of said parts check value to obtain a result; and

using said result as said contents check value.

136. (AMENDED) A recording medium recorded with a computer program for executing data processing on contents data supplied via a recording medium or a communication medium, said computer program comprising:

generating a contents check value in units of contents block data included in said contents data; and

executing collation processing on said contents check value and thereby executing verification processing as to the validity of said units of contents block data.

137. (AMENDED) A data processing apparatus for generating storing data with respect to a device for recording content data, said content data including a plurality of content blocks and a header section, at least a part of said plurality of content blocks being encrypted and said header section being operable to store information on said contents blocks, said content data being structured by encryption key data Kdis[Kcon] stored in said header section, said encryption key data Kdis[Kcon]being formed by applying an encryption key Kdis to an encryption key Kcon, said data processing apparatus comprising:

means for removing said encryption key data Kdis[Kcon] from said header section;

means for executing decryption processing on said encryption key data Kdis[Kcon] to generate decryption data Kcon;

means for generating new encryption key data Kstr[Kcon] by applying an encryption key Kstr to said decryption data Kcon;

means for storing said new encryption key data Kstr[Kcon] in said header section; and

means for applying a different encryption key Kstr to said decryption data Kcon to execute encryption processing.

138. (AMENDED) A data processing apparatus for generating storing data with respect to a device for recording content data, said content data including a plurality of content blocks and a header section, at least a part of said plurality of content blocks being encrypted and said header section being operable to store information on said content blocks, said plurality of content blocks being composed of contents encrypted by an encryption key Kblc and encryption key data Kcon[Kblc], said encryption key data Kcon[Kblc] being formed

by applying an encryption key Kcon to said encryption key Kblc, and said plurality of content blocks having a structure in which encryption key data Kdis[Kcon] is stored in said header section, said encryption key data Kdis[Kcon] being formed by applying an encryption key Kdis to said encryption key Kcon, said data processing apparatus comprising:

means for removing said encryption key data Kdis[Kcon] from said header section;

means for executing decryption processing on said encryption key data Kdis[Kcon] to generate decryption data Kcon;

means for generating new encryption key data Kstr[Kcon] by applying an encryption key Kstr to said decryption data Kcon;

means for storing said new encryption key data Kstr[Kcon] in said header section of said content data; and

means for applying a different encryption key Kstr to said decryption data Kcon to execute encryption processing.

139. (AMENDED) A data processing apparatus for generating storing data with respect to a device for recording content data, said content data including a plurality of content blocks and a header section, at least a part of said plurality of content blocks being encrypted and said header section being operable to store information on said plurality of content blocks, said plurality of content blocks being composed of contents encrypted by an encryption key Kblc and encryption key data Kdis[Kblc], said encryption key data Kdis[Kblc] being formed by applying an encryption key Kdis to said encryption key Kblc, said data processing apparatus comprising:

means for removing said encryption key data Kdis[Kblc] from a content block section;

means for executing decryption processing of said encryption key data Kdis[Kblc] to generate decryption data Kblc;

means for generating encryption key data Kstr[Kblc] by applying an encryption key Kstr to said decryption data Kblc;

means for storing said encryption key data Kstr[Kblc] in said content block section; and

means for applying a different encryption key Kstr to said decryption data Kblc to execute encryption processing.

140. (AMENDED) A content data generating method for generating content data, comprising:

coupling a plurality of content blocks including at least one of voice information, image information and program data;

applying encryption processing to at least a part of said content blocks using an encryption key Kcon;

generating encryption key data Kdis[Kcon] by applying an encryption key Kdis to said encryption key Kcon;

storing said encryption key Kdis in a header section of said content data; and

generating said content data including said plurality of content blocks and said header section.

141. (AMENDED) The content data generating method according to Claim 140, further including:

generating block information that stores at least one of:

identification information on said content data,

usage policy information including a data length of said content data and a data type of said content data,

a data length of at least one of said content blocks, and

a presence or absence of encryption processing; and

storing said block information in said header section.

142. (AMENDED) The content data generating method according to Claim 140, further including:

generating a part check value based on a portion of information composing said header section;

storing said part check value in said header section;

generating a total check value based on said part check value; and

storing said total check value in said header section.

143. (AMENDED) The content data generating method according to Claim 142, wherein said steps of generating said part check value and generating said total check value are executed by applying a DES encryption processing algorithm using data to be checked as a message and using a check value generation key as an encryption key.

144. (AMENDED) The content data generating method according to Claim 141, further including:

applying said encryption processing to said block information by applying said encryption key Kdis to an encryption key Kbit to form encryption key data Kdis[Kbit]; and

storing said encryption key data Kdis[Kbit] in said header section.

145. (AMENDED) The content data generating method according to Claim 140, wherein each of said plurality of content blocks is generated as a common fixed data length.

146. (AMENDED) The content data generating method according to Claim 140, wherein each of said plurality of content blocks is generated with an encryption data section and a non-encryption data section arranged regularly.

147. (AMENDED) A content data generating method for generating content data, comprising:

coupling a plurality of content blocks each including at least one of voice information, image information and program data;

composing at least a part of said plurality of content blocks by applying an encryption key Kcon to an encryption key Kblc to obtain encryption key data Kcon[Kblc];

generating encryption key data Kdis[Kcon] by applying an encryption key Kdis to said encryption key Kcon; and

storing said encryption key data Kdis[Kcon] in a header section of said content data; and

generating said content data including said plurality of content blocks and said header section.

148. (AMENDED) A content data generating method for generating content data, comprising:

coupling a plurality of content blocks each including at least one of voice information, image information and program data;

composing at least a part of said plurality of content blocks by applying an encryption key Kdis to an encryption key Kblc to obtain encryption key data Kdis[Kblc]; and

generating said content data including said plurality of content blocks and a header section of said content data.

149. (AMENDED) A data processing method for storing content data in a recording device, said content data having a plurality of content blocks and a header section, at least a part of said plurality of content blocks being encrypted and said header section being operable to store information on said plurality of content blocks, said content data being structured by encryption key data Kdis[Kcon] stored in said header section, said encryption key data Kdis[Kcon] being formed by applying an encryption key Kdis to an encryption key Kcon, said method comprising:

removing said encryption key data Kdis[Kcon] from said header section;

executing decryption processing on said encryption key data Kdis[Kcon] to generate decryption data Kcon;

generating new encryption key data Kstr[Kcon] by applying an encryption key Kstr to said decryption data Kcon;

storing said new encryption key data Kstr[Kcon] in said header section; and

storing said header section in said recording device together with said plurality of content blocks.

150. (AMENDED) A data processing method for storing content data in a recording device, said content data having a plurality of content blocks and a header section, at least a part of said plurality of content blocks being encrypted and said header section being operable to store information on said plurality of content blocks, said plurality of content blocks being composed of contents encrypted by an encryption key Kblc and encryption key data Kcon[Kblc], said encryption

key data Kcon[Kblc] being formed by applying an encryption key Kcon to said encryption key Kblc, and said plurality of content blocks having a structure in which encryption key data Kdis[Kcon] is stored in said header section, said encryption key data Kdis[Kcon] being formed by applying an encryption key Kdis to said encryption key Kcon, said method comprising:

removing said encryption key data Kdis[Kcon] from said header section;

executing decryption processing on said encryption key data Kdis[Kcon] to generate decryption data Kcon;

generating new encryption key data Kstr[Kcon] by applying an encryption key Kstr to said decryption data Kcon;

storing said new encryption key data Kstr[Kcon] in said header section; and

storing said header section in said recording device together with said plurality of content blocks.

151. (AMENDED) A data processing method for storing content data in a recording device, said content data having a plurality of content blocks and a header section, at least a part of said plurality of content blocks being encrypted, and said header section being operable to store information on said plurality of content blocks, said plurality of content blocks being composed of contents encrypted by an encryption key Kblc and encryption key data Kdis[Kblc], said encryption key data Kdis[Kblc] being formed by applying an encryption key Kdis to said encryption key Kblc, said method comprising:

removing said encryption key data Kdis[Kblc] from a content block section;

executing decryption processing of said encryption key data Kdis[Kblc] to generate decryption data Kblc;

generating encryption key data Kstr[Kblc] by applying an encryption key Kstr to said decryption data Kblc;

storing said encryption key data Kstr[Kblc] in said content block section; and

storing said content block section in said recording device together with said plurality of content blocks.

152. (AMENDED) A recording medium recorded with a computer program for generating storing data with respect to a device for recording content data, said content data including a plurality of content blocks and a header section, at least a part of said plurality of content blocks being encrypted and said header section being operable to store information on said contents blocks, said content data being structured by encryption key data Kdis[Kcon] stored in said header section, said encryption key data Kdis[Kcon] being formed by applying an encryption key Kdis to an encryption key Kcon, said computer program comprising:

removing said encryption key data Kdis[Kcon] from said header section;

executing decryption processing on said encryption key data Kdis[Kcon] to generate decryption data Kcon;

generating new encryption key data Kstr[Kcon] by applying aan encryption key Kstr to said decryption data Kcon; and

storing said new encryption key data Kstr[Kcon] in said header section.

153. (AMENDED) A data processing apparatus for reproducing content data, said content data including compressed contents and an expansion processing program of said compressed contents, and being provided by a storage medium or a

communication medium, said data processing apparatus comprising:

a content data analyzing section for executing content data analysis of said compressed contents and said expansion processing program of said compressed contents, and being operable to extract said compressed contents and said expansion processing program from said content data; and

an expansion processing section for executing expansion processing of said content data using said expansion processing program.

154. (AMENDED) The data processing apparatus according to Claim 153, further including:

a data storing section for storing said compressed contents; and

a program storing section for storing said expansion processing program, wherein said expansion processing section has a configuration for executing said expansion processing with respect to said compressed contents by applying said expansion processing program to said compressed contents.

155. (AMENDED) The data processing apparatus according to Claim 153, wherein said content data analyzing section has a configuration for obtaining configuration information of said content data based on header information included in said content data, and said content data analyzing section is operable to perform analysis of said content data.

156. (AMENDED) The data processing apparatus according to Claim 155, wherein:

reproduction priority information of said compressed contents is included in said header information; and

if there are a plurality of compressed contents, said expansion processing section has a configuration for

sequentially executing content expansion processing in accordance with said reproduction priority information.

157. (AMENDED) The data processing apparatus according to Claim 153, further including:

displaying means for displaying information of said compressed contents; and

inputting means for inputting reproduction contents identification data selected from said information displayed on said displaying means, wherein said expansion processing section has a configuration for executing said expansion processing of said compressed contents corresponding to said reproduction contents identification data.

158. (AMENDED) A data processing apparatus for reproducing content data, said content data including one of compressed contents and an expansion processing program, and said content data being provided by a storage medium or a communication medium, said data processing apparatus comprising:

a content data analyzing section for receiving said content data, said content data analyzing section being operable to distinguish whether said content data includes said compressed contents or said expansion processing program from header information included in said received content data;

if said content data includes said compressed contents, said content data analyzing section being operable to analyze a type of compressing processing program applied to said compressed contents from said header information;

if said content data includes said expansion processing program, said content data analyzing section being operable to analyze a type of expansion processing program from said header information; and

an expansion processing section for executing expansion processing of said compressed contents, said expansion processing section having a configuration for selecting a specific expansion processing program applicable to said type of compression processing program based on said type of expansion processing program, and being operable to execute said expansion processing by using said specific expansion processing program.

159. (AMENDED) The data processing apparatus according to Claim 158, further including:

a data storing section for storing said compressed contents analyzed by said content data analyzing section; and

a program storing section for storing said specific expansion processing program, wherein said expansion processing section has a configuration for executing said expansion processing by applying said specific expansion processing program to said compressed contents.

160. (AMENDED) The data processing apparatus according to Claim 158, further including:

reproduction priority information associated with said compressed contents, said reproduction priority information being included in said header information; and

if there are a plurality of compressed contents, said expansion processing section has a configuration for sequentially executing said expansion processing in accordance with said reproduction priority information.

161. (AMENDED) The data processing apparatus according to Claim 158, further including:

retrieving means for retrieving said specific expansion processing program; and

program storing means accessible by said data processing apparatus as an object of retrieval.

162. (AMENDED) The data processing apparatus according to Claim 158, further including:

displaying means for displaying information of said compressed contents; and

inputting means for inputting reproduction contents identification data selected from said information displayed on said displaying means, wherein said expansion processing section has a configuration for executing said expansion processing of said compressed contents corresponding to said reproduction contents identification data.

163. (AMENDED) A data processing method for reproducing content data, said content data including compressed contents and an expansion processing program of said compressed contents, said content data being provided by a storage medium or a communication medium, said method comprising:

executing content data analysis of said content data and contents;

extracting said compressed contents and said expansion processing program from said content data; and

executing expansion processing of said compressed content using said expansion processing program.

164. (AMENDED) The data processing method according to Claim 163, further including:

storing said extracted compressed contents; and

storing said extracted expansion processing program, wherein said expansion processing is executed with respect to said compressed contents by applying said expansion processing program to said compressed contents.

165. (AMENDED) The data processing method according to Claim 163, further including:

obtaining configuration information of said content data based on header information included in said content data prior to executing said content data analysis.

166. (AMENDED) The data processing method according to Claim 165, wherein:

said compressed contents includes reproduction priority information included in said header information; and

if there are a plurality of compressed contents , said expansion processing step sequentially executes content expansion processing in accordance with said reproduction priority information.

167. (AMENDED) The data processing method according to Claim 163, further including:

displaying information of said compressed contents ; and

inputting reproduction contents identification data selected from said display and information, wherein said expansion processing is performed corresponding to said reproduction contents identification data.

168. (AMENDED) A data processing method for reproducing content data, said content data including one of compressed contents and an expansion processing program, said content data being provided by a storage medium or a communication medium, said method comprising:

receiving said content data;

distinguishing whether said content data includes said compressed contents or said expansion processing program from header information included in said received content data;

if said content data includes said compressed contents, analyzing a type of compressing processing program applied to said compressed contents from said header information;

if said content data includes said expansion processing program, analyzing a type of expansion processing program from said header information;

selecting a specific expansion processing program applicable to said type of compression processing program based on said type of expansion processing program; and

executing expansion processing using said specific expansion processing program.

169. (AMENDED) The data processing method according to Claim 168, further including:

storing said compressed contents; and

storing said specific expansion processing program, wherein said expansion processing step is executed by applying said specific expansion processing program to said compressed contents.

170. (AMENDED) The data processing method according to Claim 168, wherein:

reproduction priority information is associated with said compressed contents, said reproduction priority information being included in said header information; and

if there are a plurality of compressed contents, said expansion processing step including sequentially executing said expansion processing in accordance with said reproduction priority information.

171. (AMENDED) The data processing method according to Claim 168, further including:

retrieving said specific expansion processing program from a program storing means accessible as an object of retrieval.

172. (AMENDED) The data processing method according to Claim 168, further including:

displaying information of said compressed contents ; and

inputting reproduction contents identification data selected from said displayed information, wherein said expansion processing is performed on said compressed contents corresponding to said reproduction contents identification data.

173. (AMENDED) A content data generating method for generating content data, said content data being provided by a storage medium or a communication medium, comprising:

combining compressed contents and an expansion processing program; and

generating said content data including said compressed contents and said expansion processing program.

174. (AMENDED) The content data generating method according to Claim 173, further including:

adding configuration information as header information of said content data.

175. (AMENDED) The content data generating method according to Claim 173, wherein said header information includes reproduction priority information of contents included in said content data.

176. (AMENDED) A content data generating method for generating content data, said content data being provided by a

storage medium or a communication medium, said method comprising:

identifying whether said content data has, as header information, compressed contents or an expansion processing program;

if said content data has said compressed contents, applying a type of compression processing program to the said compressed contents as header information; and

if said content data has said expansion processing program, adding a type of expansion processing program as header information.

177. (AMENDED) The content data generating method according to Claim 176, further including:

adding reproduction priority information as header information of said content data.

178. (AMENDED) A recording medium recorded with a computer program for reproducing content data, said content data including compressed contents and an expansion processing program for said compressed contents, and said content data being provided by a storage medium or a communication medium, said computer program comprising:

executing content data analysis of said content data;

extracting said compressed contents and said expansion processing program from said content data; and

executing expansion processing of said extracted content data using said extracted expansion processing program.